Study on Computer Virus Management and Precaution

Juan Wan

Xi'an Peihua University, Xi'an, Shaanxi, 710125, China

Keywords: Computer; virus; management; precaution.

Abstract: With more and more extensive application of computer in daily life of modern people, the precaution form of computer virus continues to change. Even computer virus attack events happen every day, which greatly impacts computer system and network security. The largest security threat to the computer is computer virus. Based on defining computer virus, this paper discusses distinct characteristics of computer virus, elaborates computer network security and proposes precaution strategies and management thought for computer virus.

1. Introduction

The great development of computer technology brings great convenience for people's life and work. However, computer virus as an important product of information age results in serious losses to destructions to computer resource with the emergence and spreading of computer virus. It may even trigger the tremendous disaster. In recent years, the development of internet technology has led to great acceleration of computer virus transmission, and the threat to people also becomes larger and larger. The events of computer virus infection and attack are countless. Thus, it is urgent to deeply study computer virus management and precaution.

2. Definition of computer virus

There are multiple statements on the definition of computer virus, and the meaning can be indicated from different perspectives. Three statements are listed here. Firstly, computer virus refers to a computer program or command which can result in faults. It is often put into computer operating system intentionally or unwittingly by software designers. Then, the computer program or command will implement self-replication, enter computer hard disk and infect other systems, thus leading to gross error of computer data or file and the inability of normal use. Secondly, virus spreads through magnetic tape, disk or network, duplicates and spreads the programs with infectivity, destruction and latency features through certain carriers. Besides, it can fast infect other computer programs. Thirdly, the artificial program lurks in computer programs or various forms of storage media. As long as the change comes, it will duplicate by itself, thus leading to all kinds of damages to computer resource. Thus, computer virus is the command set or program which can destruct computer resource. It can lurk in computer media for a long term through some methods. As long as the conditions are met, it can be activated to destruct the computer.

3. Distinct characteristics of computer virus

Firstly, rapidity. Like virus in medical field, computer virus has very fast speed, without rules. Since virus is mostly combined with internet and computer, as long as virus is invaded into the computer, virus will spread all kinds of viruses through multiple invasion forms such as webpage, system bug and LAN, and the spreading sped is very fast. For example, worm virus can send out over 100 virus-containing emails within 30s. After 45s, American control center can receive the infected emails as many as 38 times. Some viruses spread by computer system bugs. Sasser worm virus can infect nearly 20 million of computers within 8 days.

Secondly, destructiveness. With the rapid development of internet technology, various viruses

  DOI: 10.25236/systca.18.086

with strong destructiveness become more and more. In addition, the virus is not just the single virus, but the mixed virus which combines numerous viruses. Its killing capacity becomes stronger, and the destructiveness is also larger. For instance, MELISSA mixed virus will not just lead to computer system crash, but also will filch data of the computer infected by virus and result in data loss. Some computer systems will even controlled by hackers and lead to imponderable losses. If the virus invades into the computer and spreads online, it is hard to control the process. This is because once the system detects the virus and adopts protection measures, the virus actually has carried out large-scale replication. At this moment, the antivirus program cannot work.

Thirdly, parasitism. Computer virus is often parasitized in the program that people cannot find easily. It can't be found easily before the computer user starts the program. But when the program is executed, the virus may generate destruction effect.

Fourthly, latency. Virus can lurk through two different patterns of manifestation. The first pattern is that: computer virus remains in the tap or disk for a long time, but it will multiply quickly when the conditions are met. After replication and spreading, it will continue to engager computer system. The second pattern is that: all kinds of graphs, information or special identifications are shown in the computer screen, with the purpose of further destroying the infected computer system.

Fifthly, stealthiness. Computer virus owns very strong stealthiness. It is concealed in normal procedures, and it is hard to find. Even if the antivirus program is used, residual virus may exist, thus leading to the risk of destruction.

Sixthly, ignitionability. To hide itself and maintain the killing force, computer virus must own ignitionability. The virus will act less or even not act in order to hide itself, so the killing force is lost. Ignitionability of computer virus is used to control virus infection frequency.

4. Security of computer network

At present, security problem of computer network usually comes from internal and external network management. ISO defines computer security as follows: relevant management modes, technical means and measures are applied to make sure computer software, hardware and relevant data are not changed and destroyed at will, or revealed illegally so as to let computer network system operate continuously and stably, play a greater role and serve users. Computer security mainly covers physical security and logic security, and refers to protection of computer information confidentiality, integrity and usability. Network security refers to protection of computer information confidentiality, integrity and usability.

5. Computer virus precaution strategies

Firstly, firewall. The technology mainly applies software and hardware of computer to establish security gateway among internal and external of network as well as each department so as to avoid the attack by illegal users. In general, the isolation method can be used to distinguish internal network and public network. The authorized access is allowed and non-authorized invasion is refused to form the first defense for hacker invasion and protect computer security.

Secondly, encryption technique. The technology conducts corresponding encryption transformation of original file or data according to the corresponding algorithm, that is, implement encryption for storage and transmission. After the information user decodes the information, relevant data can be used. Usually, encryption algorithms are classified into two types: asymmetric encryption algorithm and symmetrical encryption algorithm. The keys to the both are not identical. Relatively speaking, the former is more widely used, while the decoding key of the latter is same.

Thirdly, workstation technology. There are many methods to prevent computer virus. Prevention and treatment should be first implemented at the level of workstation. Firstly, software prevention and treatment should be implemented. The essence is to apply anti-virus program to inspect computer security; secondly, install anti-virus card to avoid the trouble of manually starting antivirus program and carry out self-inspection of virus. Thirdly, install anti-virus chip on computer network interface

card to well control the workstation and effectively prevent virus infection to the computer. Meanwhile, this can well protect server and workstation, but the defect will lead to the decline of computer speed, and affect further upgrade of computer software.

Fourthly, software bug repair technology. For various kinds of software downloaded in the computer, computer users often clear rubbish of relevant software and repair the bugs at a regular interval, but Trojan maker will utilize this opportunity to find out the security bugs of the software and then invade in the software. For example, after Baidu, CorePlayer and Flash are infected by viruses, the computer use will be affected, and adverse effect will be caused to software users. Thus, before the software is used, it is required to update and repair the bugs in time and avoid manipulable space provided by software bugs for lawbreakers.

Fifthly, amend registry sheet. To attack computer system, the virus must own corresponding conditions. Like cancer cells in human body, only when they are activated can they spread. If there is no starting condition, the computer will not be infected by the virus. To prevent the emergence of the condition, the computer registry sheet should be modified in time to prevent virus invasion. For example, parasitic virus in USB will automatically recognize and invade in USB, and then load corresponding virus program, thus leading to USK damage. In such case, it is just necessary to modify registry sheet in time to prevent computer virus invasion.

6. Management thought for computer virus

Firstly, to improve security management system of computer network. Computer security should not just be protected by technology and software. It is necessary to formulate relevant management regulations on security management of computer network. In particular, there should be corresponding punishment laws and regulations. Only in this way, computer virus management and control can be based on the evidence so that personal computer network has sufficient security assurance.

Secondly, to enhance information security awareness of computer users. In most regions of China, computer knowledge education starts from middle school. However, most computer network technology education in middle school stage is dominated by theoretical knowledge education of computer, and the knowledge about virus prevention and security transfer is very little. Thus, the author considers it is required to continuously enhance users' awareness of computer virus and security defense in computer education process. Especially, computer security of staffs in enterprises and public institutions should be enhanced. Because these staffs often use computer in daily work, staffs' consciousness of handling and preventing common computer virus should be enhanced continuously. Of course, computer network management workers and program designers should cognize the importance of securely for enterprises and public institutions, and understand their duties and obligations. Meanwhile, it is required to strengthen publicity and education of computer users for computer virus, and let every computer user overall and accurately know the serious harm of virus and improve email address and password security. For unclear files received, they cannot be opened at will, and the problematic emails should be deleted in time to minimize the possibility of computer virus spreading via email. Moreover, the business ability and management work of computer professionals should be enhanced.

Thirdly, to ensure physical security of computer system. Except technical means, scientific and effective protection of environment in computer room should be implemented. The temperature, air humidity and pest disasters in computer room as well as interference and impact caused by electric magnetic field should be strictly controlled. The site f computer room should be chosen rationally. For example, in telecom enterprises, since the number of computers in customer service center is large, the structure of computer room is quite complex. Based on the above conditions, the computer room should be arranged far away from other computer groups. Besides, the temperature in the room cannot be too high, and there is also no disturbance of electromagnetic field due to air conditioner and other relevant devices. Naturally, the computer room should not be arranged in the serious noise area and under high-rise buildings or water bust equipment. The purpose is to manage the entrance of

computer room and prevent damages by lawbreakers. Of course, multi-level security protection areas should be arranged for computer room control system, and the computer room should own the ability to resist illegal violent invasion. In addition, it is required to enhance strict management and control of computer network, formulate thorough management mechanism and carefully execute it so as to prevent physical and artificial destructions.

7. Conclusions

In conclusion, in view of rapid development of modern network technology, its application scope becomes wider and wider, and meanwhile evolution and transmission speed of computer virus become faster. To better prevent the emergence of new viruses, control virus variant in time, keep clear network and make sure cloud security of computer system has become the main link of computer system security, it is required to improve the cognition for computer security and create secure computer application environment with the continuous progress of network technology.

References

[1] Du Yun, On key problem and precaution measures of cloud computing security, *Electronic Technology and Software Engineering*, 2016 (3).

[2] Hu Haifeng, On computer virus and general control methods, *Vocational Technology*, 2016 (8).

[3] Zhou Hongbo, Introduction to computer virus defense measures and key elimination points in the era of information technology, *Technology Outlook*, 2016 911).

[4] Tan Liubin, Correct defense of computer virus, *Computer Knowledge and Technology*, 2016 (20).

[5] Li Ting, Features and prevention of computer virus, *Wireless Internet Technology*, 2017 (7).

[6] Ma Lili, Computer virus and precaution, *Science & Technology Information*, 2017 (23).